UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/786,160	02/26/2004	Hirotaka Yoshida	62807-167	9154

7590 09/28/2007

MCDERMOTT, WILL & EMERY
600 13th Street, N.W.
Washington, DC 20005-3096

EXAMINER	
BAYOU, YONAS A	
ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
09/28/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/786,160	YOSHIDA ET AL.	
	Examiner	Art Unit	
	Yonas Bayou	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *02/08/2005 and 07/19/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1- 23 are rejected under 35 U.S.C. 102(b) as being anticipated by Gligor et al., Pub. No. US 2002/0048364 A1 (hereinafter Gligor).

Referring to claims 1, 13 and 21, Gligor teaches a program-storing medium and an encryption apparatus for a common-key cipher, comprising:

a unit for generating a plurality of plaintext blocks Pi (1<=i<=N) resulting from separating a plaintext on a specific-length basis, the plaintext including redundant data and a message **[paragraph 67];**

an encryption operation unit for generating a random-number string R from a secret key **[paragraph 47-48 and paragraph 160, lines 16-35;** E1=r0**],**

generating random-number blocks Ri (1<=i<=N+1) from the random-number string R **[paragraph 160, lines 30-35]** and

performing an encryption operation for ciphertext blocks Ci (1<=i<=N+2) by using the plaintext blocks Pi (1<=i<=N) and the random-number blocks Ri

(1<=i<=N+1), the random-number string R being longer than the plaintext, the random-number blocks Ri (1<=i<=N+1) being used for the encryption corresponding to the plaintext blocks Pi (1<=I<=N) **[paragraph 163;** hidden corresponding to encrypted]; and

an authentication operation unit for generating random-number blocks Ri (2<=i<=N+1) from the random-number string R **[paragraph 13, lines 1-5]**, and

performing an authentication operation for message-authentication-code blocks by using the ciphertext blocks Ci (1<=i<=N+2) and the random-number blocks Ri (2<=i<=N+1), the random-number blocks Ri (2<=i<=N+1) being used for the authentication corresponding to the ciphertext blocks Ci (1<=i<=N+2) **[paragraph 12, lines 1-8, 16-23 and paragraphs 13-15;** integrity check/MDC function corresponding to MAC/ authentication operation].

Referring to claims 2 and 14, Gligor teaches a program-storing medium and an encryption apparatus for a common-key cipher, wherein

the encryption operation unit and the authentication operation unit use the one or more random-number blocks Ri (1<=i<=N+1) **[paragraph 157, lines 19-26 and fig. 1;** MDC function corresponding to authentication operation],

the total-sum length of the one or more random-number blocks Ri (1<=i<=N+1) being longer than the total-sum length of the plaintext blocks Pi (1<=i<=N), and being shorter than two times the total-sum length of the plaintext blocks Pi (1<=i<=N) **[paragraph 159;** En is derived from r_0, see claim 1b above].

Referring to claims 3 and 15, Gligor teaches a program-storing medium and an encryption apparatus for a common-key cipher, wherein

the encryption operation unit performs a binomial operation or a monomial operation one or more times in accordance with predetermined processing steps, the binomial operation or the monomial operation using the plaintext blocks Pi (1<=i<=N) **[paragraph 14]**,

the authentication operation unit performing a binomial operation or a monomial operation one or more times in accordance with predetermined processing steps, the binomial operation or the monomial operation using the ciphertext blocks Ci (1<=i<=N+2) **[paragraph 13]**,

the encryption apparatus for a common-key cipher further comprising a unit for combining the plurality of acquired ciphertext blocks Ci (1<=i<=N+2) with the message-authentication-code blocks, and outputting the combined result as a ciphertext **[paragraph 163 and fig. 1;** block 87/Z5 comprises MDC block 22 and MDC function 91/MAC].

Referring to claims 4 and 16, Gligor teaches a program-storing medium and an encryption apparatus for a common-key cipher, wherein

the encryption operation unit performs the encryption operation by an exclusive-OR logical sum **[paragraph 157, lines 7-10]**,

the authentication operation unit performing the authentication operation by an arithmetic multiplication and an arithmetic addition **[paragraphs 13 and 14]**.

Referring to claims 5 and 17, Gligor teaches a program-storing medium and an encryption apparatus for a common-key cipher, wherein

the encryption operation unit performs the encryption operation by an exclusive-OR logical sum **[paragraph 157, lines 7-10]**,

the authentication operation unit performing the authentication operation by a multiplication on a finite field and an arithmetic addition **[paragraphs 13-14 and paragraph 18, lines 1-8;** where P is a prime number].

Referring to claims 6 and 18, Gligor teaches a program-storing medium and an encryption apparatus for a common-key cipher, wherein

the encryption operation unit and the authentication operation unit share the random-number blocks Ri (1<=i<=N+1) used by the encryption operation unit and, the authentication operation unit **[paragraph 53]**.

Referring to claim 7, Gligor teaches a program-storing medium and an encryption apparatus for a common-key cipher, wherein

the encryption operation unit and the authentication operation unit use the random-number blocks Ri (1<=i<=N+1) which differ from each other **[paragraph 87]**.

Referring to claims 8 and 19, Gligor teaches a program-storing medium and an encryption apparatus for a common-key cipher, further comprising

a pseudo random-number generation unit for generating the random-number string R from said secret key **[paragraph 89]**.

Referring to claims 9 and 20, Gligor teaches a program-storing medium and an encryption apparatus for a common-key cipher, further comprising

a unit for dividing the message into a plurality of messages, the pseudo random-number generation unit generating the random-number string R whose random numbers are equivalent to the divided messages in number **[paragraph 90]**; and

a unit for allocating either of the divided messages and the random-number string R to different operation units each, and thereby causing a parallel processing to be performed **[paragraph 85]**.

Referring to claim 10, Gligor teaches a decryption apparatus for a common-key cipher, comprising:

a unit for generating a plurality of ciphertext blocks C'i (1<=i<=N+2) resulting from separating a ciphertext on a specific-length basis **[paragraph 164 and fig. 2;** y has N+2 blocks];

an authentication operation unit for

generating a random-number string R from a secret key **[paragraph 166]**,

generating random-number blocks Ri (1<=i<=N+1) from the random-number string R **[paragraph 167, lines 1-5;** E comprises r],

and

performing an authentication operation for message-authentication-code blocks by using the ciphertext blocks C'i (1<=i<=N+2) and the random-number blocks Ri (1<=i<=N+1), the random-number string R being longer than the ciphertext, the random-number blocks Ri (1<=i<=N+1) being used for the authentication corresponding to the ciphertext blocks C'i (1<=i<=N+2) **[paragraph 168]**; and

a decryption operation unit for

generating random-number blocks Ri (1<=i<=N+1) from the random-number string R **[paragraph 167, lines 1-5]**, and

performing a decryption operation for plaintext blocks P'i (1<=i<=N) by using the ciphertext blocks C'i (1<=i<=N+2) and the random-number blocks Ri (1<=i<=N+1), the random-number blocks Ri (1<=i<=N+1) being used for the decryption corresponding to the ciphertex~t blocks C'i (1<=i<=N+2) **[paragraph 168]**.

Referring to claims 11 and 22, Gligor teaches a decryption apparatus for a common-key cipher, wherein

the authentication operation unit and the decryption operation unit use the one or more random- number blocks Ri (1<=i<=N+1) **[paragraph 168, lines 1-7]**,

the total-sum length of the one or more random-number blocks Ri (1<=i<=N+1) being longer than the total-sum length of the plaintext blocks P'i (1<=i<=N), and being shorter than two times the total-sum length of the plaintext blocks P'i (1<=i<=N) **[paragraph 168;** E is longer than the total-sum length of x].

Referring to claims 12 and 23, Gligor teaches a decryption apparatus for a common-key cipher, further comprising:

a unit for connecting the plurality of plaintext blocks P'i (1<=i<=N) thereby to generate a plaintext **[paragraph 188, lines 11-13]**;

a unit for extracting redundant data included in the plaintext **[paragraph 157, lines 10-17]**; and

a unit for checking the redundant data thereby to detect the presence or absence of a forgery that may have been performed to the ciphertext **[paragraph 11, lines 11-15]**.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yonas Bayou whose telephone number is 571-272-7610. The examiner can normally be reached on m-f,7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571-272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Yonas Bayou

YB

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER